REMARKS

The claims previously indicated to be allowable are now rejected in view of the new reference to Sudia. In addition, new claims 33 and 40 were rejected under Section 102 based on Sudio.

Starting with claims 33-40, it is noted that these claims call for having a first portion of a firmware code which is not upgradeable and a second portion of a firmware code that is upgradeable and providing information for authenticating an upgrade of the second portion and a first portion. The only citation in support of the rejection is Sudia, paragraph 99, which says virtually nothing. It cannot possibly meet the claimed limitations because it does not talk about firmware, it does not talk about firmware having two different portions, and it does not talk about firmware having two different portions, one of which is upgradeable and the other which is not. Finally, it does not say anything about providing information for authenticating an upgrade of the second portion and the first portion. Reconsideration of the rejection of claim 33 is, therefore, requested. On the same basis, reconsideration of the rejection of claim 40 is requested.

Moving to claim 1, the subject matter was previously indicated to be allowable prior to citation of Sudia. However, Sudia does not teach retrieving a second public key. Instead, he simply teaches obtaining the same public key from other sources. Moreover, he does not teach retrieving a second public key from a firmware program. Finally, he does not teach retrieving a second public key "if the public key is not valid."

The cited paragraph 251 merely talks about the situation where a private key is compromised through theft. There is no validating of any public key, nor is there retrieving a public key from the firmware program if the public key is valid. The firmware program is the one that identifies the firmware upgrade request, meets the limitation of upgrading a portion of the firmware program by the firmware program and is involved in locking a device storing the firmware program, such that the second portion of the firmware program is not readable. Here, there is no validating of any public key or retrieving a different public key from a firmware program if the public key used to validate a file is not valid. Therefore, reconsideration of the rejection of claim 1 is respectfully requested.

With respect to claim 13, there is no backup public key. As explained in paragraph 251 of the reference, if the manufacturer included the replacement of its own public key among the

transactions that the third party's public instructions key could approve, the manufacturer could then turn to that trusted third party and request that it issue an instruction data packet to all the manufacturer's device authorizing a replacement of the manufacturer's public signature key. But there was no backup public key, there was simply a public key and the ability to go ask someone else to permit replacement of that manufacturer's public signature key.

Therefore, reconsideration is requested.

With respect to claim 19, the present application and the cited patent 6,711,675 were, at the time the invention of the present application was made, owned by Intel Corporation.

Therefore, under Section 103, the rejection of claim 19 should be reconsidered.

Respectfully submitted,

Date: April 20, 2006

Timothy N. Trop, Reg. No. 28,994
TROP, PRUNER & HU, P.C.
8554 Katy Freeway, Ste. 100
Houston, TX 77024
713/468-8880 [Phone]
713/468-8883 [Fax]

Attorneys for Intel Corporation